Brussels, March 2025

BSP Position Paper: Digital Omnibus – feedback

Business & Science Poland

This position paper is submitted on behalf of Business & Science Poland (BSP) *in response to the European Commission's Proposal for a regulation - COM(2025)836 on the "Digital Omnibus" (Digital Package on Simplification). It addresses simplification proposals drawn from industry experience.*

Background

Business & Science Poland (BSP) welcomes the European Commission's proposal for the Digital Omnibus, introduced as part of the broader simplification agenda. The initiative represents a timely effort to rationalise elements of the EU's increasingly complex digital regulatory framework. Efforts to streamline existing legislation and improve coherence across the digital rulebook are particularly valuable at a time when businesses and public authorities alike face growing regulatory fragmentation. In this context, the consolidation and repeal of certain overlapping provisions may nonetheless contribute to greater legal clarity and more consistent application of EU law across the Single Market.

The initiative also addresses a long-standing challenge within the current data protection framework: the widespread phenomenon of "consent fatigue" generated by the proliferation of GDPR consent notices that interrupt users' online experience without necessarily enhancing their understanding or control. By seeking to simplify these mechanisms and improve their practical functioning, the Commission rightly acknowledges the need to make the EU's digital regulatory environment both more user-friendly and more effective.

At the same time, while the proposal represents a positive step towards regulatory simplification, further reflection and targeted improvements would help ensure that its objectives are fully achieved. Building on the Commission's work, the considerations outlined in the accompanying policy contributions highlight several areas where additional clarification and refinement could strengthen legal certainty, enhance coherence, and better reflect technological and market realities. In particular, attention should be given to ensuring consistent enforcement mechanisms, reducing unnecessary consent requirements for low-risk activities, and providing clearer and more harmonised legal standards for emerging technologies such as artificial intelligence.

Taken together, these considerations suggest that the Digital Omnibus offers an important opportunity not only to simplify existing legislation but also to promote a more

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89

coherent, operationally workable and innovation-friendly digital framework across the European Union.

Key BSP recommendations

- Provide predictable regulatory timelines for high-risk AI systems;
- Preserve the risk-based structure of the AI Act;
- Strengthen legal certainty within the GDPR framework;
- Resolve the enforcement fragmentation between GDPR and ePrivacy rules;
- Address consent fatigue through broader exemptions for low-risk processing
- Adopt the "report once, comply with many" principle for incident notifications with harmonised thresholds, definition, timelines;
- Address overlaps within the EU digital acquis through the Digital Fitness Check.

Practical experience - expert remarks

To ensure that the present feedback reflects practical experience and expert perspectives, the commentary below builds on the outcomes of an expert roundtable discussion organised by Business & Science Poland (BSP) and the CEE Digital Coalition on 25 February. The event *"Digital Omnibus: Simplification of EU regulations and their impact on Poland and the CEE region"*, brought together representatives of industry associations, companies, policy experts and stakeholders from across the digital ecosystem.

The roundtable aimed to examine the European Commission's Digital Omnibus proposal from the perspective of businesses and experts operating within the EU digital economy. Participants discussed whether the initiative can effectively simplify the increasingly complex digital regulatory framework while preserving high standards of security, data protection and consumer trust.

The discussion focused in particular on three areas: **implementation of the Artificial Intelligence Act, the interaction between the GDPR and ePrivacy rules, and the simplification of cybersecurity obligations**. Experts shared practical experiences with the existing regulatory framework and discussed how the Omnibus could better address regulatory overlaps, legal uncertainty and administrative burdens affecting European businesses.

The observations presented below summarise the main conclusions emerging from this expert discussion. They complement and further develop the recommendations

previously outlined in the **BSP position paper on the Digital Omnibus**, submitted in response to the European Commission's call for evidence.

Artificial Intelligence:

AI Act implementation timelines

Participants emphasised that the implementation schedule of certain AI Act obligations may not sufficiently reflect the practical realities faced by businesses preparing for compliance.

A significant part of the discussion focused on the feasibility of the current timeline for the implementation of the Artificial Intelligence Act, particularly regarding transparency obligations under Article 15. Several participants noted that important implementation tools, including the Code of Practice, are expected to be finalised only around June 2026, leaving companies with a very limited timeframe to adapt their systems before the relevant obligations apply in August 2026. This short transition period was widely viewed as insufficient for organisations to introduce the necessary technical and organisational adjustments.

Participants therefore underlined the need to better align regulatory deadlines with the availability of practical guidance and implementation standards. In this context, several speakers suggested extending the compliance period for Article. Some contributors also suggested that a broader pause in the implementation timeline could allow regulators and industry additional time to evaluate the framework and introduce targeted improvements where necessary.

Predictability for high-risk AI systems

Participants stressed that clearer and more predictable application dates are essential for effective compliance planning.

The discussion also addressed the regulatory timeline for high-risk AI systems, with participants emphasising the importance of legal certainty in this area. Rather than relying on conditional or flexible deadlines dependent on administrative decisions, several speakers suggested that the Digital Omnibus could introduce clear and fixed application dates for obligations related to high-risk systems listed in Annex III and Annex I of the AI Act. Establishing such deadlines was considered beneficial in providing companies with a stable planning horizon and enabling more effective preparation for compliance with the regulatory requirements.

Scope of high-risk AI classification

Ensuring that the AI Act preserves its risk-based structure was identified as an important regulatory priority.

Participants also raised concerns regarding the interpretation of Article 6 of the AI Act, which defines the classification of high-risk AI systems. Some speakers warned that an overly broad interpretation of this provision could potentially result in a wide range of products incorporating relatively limited AI functionality being classified as high-risk.

Examples mentioned included consumer products such as household appliances that incorporate basic AI features. Participants argued that if such products were systematically categorised as high-risk, this could undermine the risk-based logic that forms the foundation of the AI Act. Maintaining a targeted and proportionate classification framework was therefore considered essential to ensure that regulatory obligations remain aligned with the actual level of risk associated with specific AI applications.

GDPR and ePrivacy:

Regulatory complexity and fragmentation

The interaction between the GDPR and the ePrivacy framework was identified as the most complex and debated aspect of the Digital Omnibus proposal.

While participants consistently reaffirmed their support for the EU's strong data protection standards, many also highlighted growing concerns about legal uncertainty and fragmentation in the application of the General Data Protection Regulation (GDPR) across Member States. Speakers pointed to divergent interpretations by national data protection authorities and evolving jurisprudence that have expanded the interpretation of key concepts, including the definition of personal data and the scope of special categories of data.

Strengthening proportionality in GDPR enforcement

Participants highlighted the importance of ensuring that the GDPR operates according to a clear risk-based and proportionate approach.

Several speakers emphasised that the regulatory framework could benefit from clearer guidance on the application of concepts such as legitimate interest, as well as a reduction in duplicative documentation requirements that create administrative burdens without necessarily improving data protection outcomes. Participants also discussed the need for a more practical approach to handling data access requests, which companies often experience as highly resource-intensive.

Particular attention was devoted to the treatment of pseudonymised data, which was identified as an area where additional clarification could help reduce legal uncertainty while maintaining appropriate safeguards for individuals.

Addressing consent fatigue

Participants broadly agreed that the current cookie consent regime creates significant usability challenges for both users and businesses.

The issue of **consent fatigue** emerged as a recurring theme during the discussion. Participants noted that users are frequently confronted with numerous consent banners and privacy notices while browsing the internet, often leading them to accept or reject options without fully considering the implications.

In this context, the Digital Omnibus was seen as an opportunity to reconsider how consent mechanisms function in practice. Several speakers suggested that consent requirements should focus on genuinely high-risk processing activities, while routine or low-risk uses such as certain security, analytics or contextual advertising functions could potentially be addressed through more proportionate regulatory mechanisms.

Detailed proposals - legal certainty and coherence in the GDPR framework

Ensure a single, harmonized standard for AI and legitimate interest	
Proposed change	**Justification**
The proposed Article 88c—which confirms legitimate interest as an appropriate legal basis for AI training and operation—is highly positive for any company developing or fine-tuning models in Europe. It offers significantly greater legal certainty than the December 2024 EDPB Opinion for companies to base their entire legal compliance on. However, the current drafting undermines these benefits by imposing new conditions that diverge from standard GDPR rules for legitimate interest.	To ensure legal certainty and prevent Single Market fragmentation, Article 88c must be harmonized with established GDPR case law. Therefore, the provision allowing Member States to impose national consent requirements and opening the door to 27 different or contradicting national regimes should be deleted. A unified and predictable framework is essential for cross-border digital services and AI development within the EU. Co-legislators should additionally ensure the conditions for legitimate interest are harmonised between AI development and other processing activities as recommended by the EDPB/EDPS Joint Opinion. We recommend deleting the additional conditions in Article 88c to ensure the test remains consistent for all technologies. As a final point, the Omnibus should focus on the activity (data processing) rather than undefined labels like "AI models." Alternatively, co-legislators should reference the definition of a “general-purpose AI model” in Article 3, point (63) Regulation

	(EU) 2024/1689.
Replace the strict "avoid" obligation for special category data with a risk-based standard	
Proposed change	**Justification**
We welcome the Omnibus proposal's exception for the incidental and residual processing of special categories of data in AI. This rightly recognizes that such data is crucial for mitigating bias and ensuring necessary representativeness in AI systems. However, the current drafting attaches unworkable conditions to this exception, requiring improvement.	First, the requirement to strictly "avoid" collecting sensitive data from the open web is technically unworkable. As the EDPB/EDPS Joint Opinion explicitly notes, "it is not always possible for controllers to avoid residual and incidental processing of special categories of data.1" In practice, this obligation creates a privacy paradox: developers are forced to conduct invasive monitoring just to identify and filter out potential sensitive data. This rigid approach should be replaced with a practical "risk mitigation" standard across the AI development life cycle, grounded in appropriate technical and organisational measures like Privacy-enhancing technologies (PETs). This solution maintains the GDPR's core balance between protection and innovation, ensuring that any incidentally collected data is processed in a highly secure manner. At the same time, mandatory output filters that undermine the functional utility of AI tools such as preventing a chatbot from answering factual, public questions about a public figure's political opinions or health history should be removed. Overly restrictive obligations risk limiting the effectiveness and competitiveness of AI systems developed and deployed within the European Union.

Detailed proposals - recommendation on ePrivacy

Ensure Unified GDPR Enforcement – End the split regime	
Proposed change	**Justification**
To achieve genuine simplification and prevent enforcement fragmentation, the current "split regime: between personal and non-personal data must be resolved. Rules concerning access to and storage of information in terminal equipment should be fully integrated into the GDPR framework under a single, consistent enforcement mechanism. It is also highly politically relevant: full	Maintaining separate enforcement tracks risks regulatory inconsistency, overlapping competencies, and legal uncertainty for cross-border businesses. — a risk explicitly echoed by the regulators in the recent EDPB/EDPS Joint Opinion. A unified GDPR-based approach would ensure coherence, reduce administrative burdens, and strengthen predictability for both

integration directly supports the Commission's broader objective to streamline the digital rulebook and dismantle the outdated ePrivacy Directive by the end of this mandate.	companies and supervisory authorities. Therefore, we believe all rules concerning access to and storage of information in terminal equipment must be fully integrated into the GDPR framework under a single, consistent enforcement mechanism. This consolidation will deliver the Commission's simplification agenda without compromising security, as unauthorized access to devices remains strictly prohibited and penalized under existing national computer misuse laws.
Expand Article 88a – Make exemptions real and effective	
Proposed change	**Justification**
We agree with the Commission's assessment that the current cookie consent system is broken. Under the existing legal framework, both low-impact processing (such as contextual advertising) and high-impact behavioural profiling operations trigger the same user consent requirement. This creates a systemic disincentive for businesses to invest in and develop more privacy-oriented products, while simultaneously overwhelming users with ubiquitous consent banners. However, the current ambition of the Digital Omnibus is insufficient to address this structural problem. The two additional exemptions currently foreseen – security and audience measurement – are too narrow to meaningfully change the status quo. The Digital Omnibus presents a crucial opportunity to address two systemic issues simultaneously: reducing excessive consent banners and incentivizing privacy-by-design business models. To achieve this, Article 88a must be expanded to exempt low-risk, non-profiling activities that are essential for the functioning of the digital ecosystem.	By allowing businesses to adopt privacy-safe models without triggering consent requirements, the regulation would create a tangible market reward for privacy-by-design activities. This would simultaneously support business viability, — particularly for SMEs and publishers in Central and Eastern Europe—, while delivering the simplified user experience with far fewer banners that citizens increasingly expect. This would also align with the EU privacy regulators that explicitly invited policy-makers to exempt contextual advertising and low-impact activities (fraud, measurement and capping) from user consent "to provide an incentive to use less intrusive forms of advertising online". Therefore, expanding Article 88a to exempt contextual advertising—alongside its necessary functions like fraud prevention, measurement, and frequency capping—creates a critical and unique alignment of interests. We encourage co-legislators to adopt this approach, as it supports industry competitiveness, answers regulators' calls for privacy-centric models, and directly benefits users by reducing banner fatigue

Cybersecurity reporting and regulatory coherence

Participants broadly supported efforts to simplify existing reporting obligations.

The proposal to introduce a single entry point for cybersecurity incident reporting was generally welcomed as a practical step towards reducing administrative complexity for companies operating across multiple regulatory frameworks. However, participants emphasised that significant challenges remain due to overlapping reporting obligations arising from several EU legislative instruments, including the NIS2 Directive, the Cyber

Resilience Act (CRA), the Digital Operational Resilience Act (DORA), the AI Act and the GDPR.

Experts therefore suggested that further harmonisation would be beneficial. Proposals discussed included introducing common reporting templates, clearer definitions of reportable incidents and more consistent reporting timelines. One specific suggestion involved aligning reporting requirements around a 72 hour reporting window, with the reporting timeline beginning once an incident has been confirmed rather than merely suspected.

Conclusion

The Digital Omnibus represents an important opportunity to advance the European Commission's ambition of simplifying the Union's digital regulatory framework while preserving the high standards of protection for fundamental rights, data security and consumer trust that underpin the European model. Business & Science Poland therefore welcomes the initiative as a constructive step towards addressing the growing complexity of the EU digital rulebook and improving the coherence of its application across the Single Market.

The observations and recommendations presented in this paper illustrate that meaningful simplification will depend not only on consolidating legislation but also on ensuring that the resulting framework remains proportionate, predictable and aligned with technological realities: greater clarity in the implementation of the AIA, greater coherence in the GDPR framework, and further harmonisation of cybersecurity reporting obligations would contribute significantly to reducing unnecessary regulatory burdens while maintaining robust safeguards.

BSP also wishes to underline that the considerations outlined in this paper build upon earlier contributions submitted during the **initial Digital Omnibus consultations**, where we identified several areas in which overlapping or duplicative provisions have emerged within the evolving digital acquis. These reflections have been further developed in the context of the ongoing **Digital Fitness Check**, in which BSP has highlighted specific instances where regulatory obligations across different instruments intersect or partially overlap, creating unnecessary complexity for businesses operating across multiple jurisdictions.

Addressing such overlaps in a systematic manner will be essential if the Union's simplification agenda is to achieve its intended effect. A coherent and well-aligned digital regulatory framework would not only reduce compliance costs but also strengthen legal

certainty and support the development of innovative technologies within the European economy

About BSP

Business & Science Poland (BSP) combines the experience of leading Polish enterprises with the EU agenda. We represent the knowledge and interests of Polish companies employing over 180,000 people in Poland, the EU, and globally. Our goal is to support the EU Single Market in line with the need for its responsible and effective transformation. This opinion presents the position of BSP members representing the digital, financial, air transport, fertiliser, chemical, mining, refining, fuel and energy sectors.

Rue Belliard 40, 1000 Brussels
e-mail: info@zpbsp.com
EU Transparency Register Number: 548212735276-89